INSTALACION, CONFIGURACION E INTEGRACION DE LDAP CON OTROS SISTEMAS

Autor:
JOHNY ALEJANDRO ROJAS GONZALEZ

Tutor Investigación: CARLOS QUIJANO NARVAEZ

POLITÉCNICO COLOMBO ANDINO
FACULTAD DE ANALISIS Y DISEÑO DE SISTEMAS
BOGOTÁ D.C.
FEBRERO 2010

TABLA DE CONTENIDO

INTRODUCCION

OpenLDAP es una implementación libre y de código abierto del protocolo Lightweight Directory Access Protocol (LDAP) desarrollada por el proyecto OpenLDAP. Está liberada bajo su propia licencia OpenLDAP Public License. LDAP es un protocolo de comunicación independiente de la plataforma. Muchas distribuciones GNU/Linux incluyen el software OpenLDAP para el soporte LDAP. Este software también corre en plataformas BSD, AIX, HP-UX, Mac OS X, Solaris, Microsoft Windows (NT y derivados, incluyendo 2000, XP, Vista), y z/OS.

Básicamente, OpenLDAP posee tres componentes principales:

- slapd - Dominio de servidor y herramientas.
- Bibliotecas que implementan el protocolo LDAP.
- Programas cliente: ldapsearch, ldapadd, ldapdelete, entre otros.

OBJETIVOS

OBJETIVOS GENERALES

- Dar a conocer las ventajas y la facilidad de implementación de un sistema de Autenticación como lo es OpenLDAP.

- Mostrar a los estudiantes lo importante que puede llegar a ser para una empresa la utilización de software Libre GNU.

- Motivar la migración a nuevas plataformas informáticas utilizando las grandes herramientas que nos puede brindar el software Libre GNU.

OBJETIVOS ESPECIFICOS

- Brindar conocimientos básicos sobre la utilización y la puesta en marcha de un sistema de Autenticación y Dominio como lo es OpenLDAP.

- Apoyar de una manera didáctica los temas relacionados con OpenSUSE.

- Adquirir los conocimientos básicos sobre la instalación, configuración, administración y mantenimiento de un Servidor OpenLDAP.

1. ¿Qué es LDAP?

1.1. Descripción de LDAP

LDAP ("Lightweight Directory Acces Protocol", en español Protocolo Ligero de Acceso a Directorios) es un protocolo de tipo cliente-servidor para acceder a un servicio de directorio.

Se usó inicialmente como un Front-end o interfaz final, pero también puede usarse con servidores de directorio únicos y con otros tipos de servidores de directorio.

1.1.1. ¿Qué es un directorio?

Un directorio es una base de datos, pero en general contiene información más descriptiva y más basada en atributos. La información contenida en un directorio normalmente se lee mucho más de lo que se escribe. Como consecuencia los directorios no implementan normalmente los complicados esquemas para transacciones o esquemas de reducción que las bases de datos utilizan para llevar a cabo actualizaciones complejas de grandes volúmenes de datos.

Las actualizaciones en un directorio son usualmente cambios sencillos de todo o nada, si es que permiten algo. Los directorios están para proporcionar una respuesta rápida a operaciones de búsqueda o consulta. Pueden tener capacidad de replicar información de forma amplia, con el fin de aumentar la disponibilidad y fiabilidad, y a la vez reducir tiempo de respuesta. Cuando se duplica la información de un directorio, pueden aceptarse inconsistencias temporales entre la información que hay en las réplicas, siempre que finalmente exista una sincronización.

Hay muchas formas de proporcionar un servicio de directorio. Los diferentes métodos permiten almacenar en el directorio diferentes tipos de información, establecer requisitos diferentes para hacer referencias a la información, consultarla y actualizarla, la forma en que protege al directorio de accesos no autorizados.

Algunos servicios de directorios son locales, proporcionando servicios a un contexto restringido. Otros servicios son globales, proporcionando servicio en un contexto mucho más amplio.

1.1.2. ¿Un directorio LDAP es una base de datos?

El sistema gestor de una base de datos (Database Management System ó DBMS) de Sybase, Oracle, Informix ó Microsoft es usado para procesar peticiones (queries) ó actualizaciones a una base de datos relacional. Estas

bases de datos pueden recibir cientos o miles de órdenes de inserción, modificación o borrado por segundo.
Un servidor LDAP es usado para procesar peticiones (queries) a un directorio LDAP. Pero LDAP procesa las órdenes de borrado y actualización de un modo muy lento.
En otras palabras, LDAP es un tipo de base de datos, pero no es una base de datos relacional. No está diseñada para procesar cientos o miles de cambios por minuto como los sistemas relacionales, sino para realizar lecturas de datos de forma muy eficiente.

1.1.3. Funcionamiento de LDAP

El servicio de directorio LDAP se basa en un modelo cliente-servidor.
Uno o más servidores LDAP contienen los datos que conforman el árbol de directorio LDAP o base de datos troncal, el cliente LDAP se conecta con el servidor LDAP y le hace una consulta. El servidor contesta con la respuesta correspondiente, o bien con una indicación de donde puede el cliente hallar más información.
No importa con que servidor LDAP se conecte el cliente ya que siempre observará la misma vista del directorio; el nombre que se le presenta a un servidor LDAP hace referencia a la misma entrada a la que haría referencia en otro servidor LDAP.

1.2. Ventajas en el uso de LDAP

Un directorio LDAP destaca sobre los demás tipos de bases de datos por las siguientes características:

- Es muy rápido en la lectura de registros
- Permite replicar el servidor de forma muy sencilla y económica
- Muchas aplicaciones de todo tipo tienen interfaces de conexión a LDAP y se pueden integrar fácilmente
- Dispone de un modelo de nombres globales que asegura que todas las entradas son únicas
- Usa un sistema jerárquico de almacenamiento de información.
- Permite múltiples directorios independientes
- Funciona sobre TCP/IP y SSL
- La mayoría de aplicaciones disponen de soporte para LDAP
- La mayoría de servidores LDAP son fáciles de instalar, mantener y optimizar.

1.3. Usos prácticos de LDAP

Dadas las características de LDAP sus usos más comunes son:

- Directorios de información: Por ejemplo bases de datos de empleados organizados por departamentos (siguiendo la estructura organizativa de la empresa) ó cualquier tipo de páginas amarillas.
- Sistemas de autenticación/autorización centralizada: Grandes sistemas donde se guarda gran cantidad de registros y se requiere un uso constante de los mismos. Por ejemplo:
    - Active Directory Server de Microsoft, para gestionar todas las cuentas de acceso a una red corporativa y mantener centralizada la gestión del acceso a los recursos.
    - Sistemas de autenticación para páginas Web, algunos de los gestores de contenidos más conocidos disponen de sistemas de autenticación a través de LDAP.
    - Sistemas de control de entradas a edificios, oficinas….
- Sistemas de correo electrónico: Grandes sistemas formados por más de un servidor que accedan a un repositorio de datos común.
- Sistemas de alojamiento de páginas web y FTP, con el repositorio de datos de usuario compartido.
- Grandes sistemas de autenticación basados en RADIUS, para el control de accesos de los usuarios a una red de conexión o ISP.
- Servidores de certificados públicos y llaves de seguridad.
- Autenticación única ó “single sign-on” para la personalización de aplicaciones.
- Perfiles de usuarios centralizados, para permitir itinerancia ó “Roaming”
- Libretas de direcciones compartidas.

1.4. ¿cuándo resulta interesante usar LDAP?

Como hemos visto LDAP es una base de datos optimizada para entornos donde se realizan muchas lecturas de datos y pocas modificaciones o borrados.

Por lo tanto es muy importante saber elegir dónde es conveniente usarlo. No será conveniente como base de datos para sitios que realicen constantes modificaciones de datos (por ejemplo en entornos de e-commerce)

Normalmente el tipo de preguntas que debes hacerte para saber si LDAP es conveniente para tus aplicaciones son:

- ¿Me gustaría que los datos fueran disponibles desde distintos tipos de plataforma?
- ¿necesito acceso a estos datos desde un número muy elevado de servidores y/o aplicaciones?
- Los datos que almaceno ¿son actualizados muchas veces?, o por el contrario ¿son sólo actualizados unas pocas veces?

- ¿tiene sentido almacenar este tipo de datos en una base de datos relacional? Si no tiene sentido, ¿puedo almacenar todos los datos necesarios en un solo registro?
- Pongamos algunos ejemplos:

Sistema de correo electrónico

Cada usuario se identifica por su dirección de correo electrónico, los atributos que se guardan de cada usuario son su contraseña, su límite de almacenamiento (quota), la ruta del disco duro donde se almacenan los mensajes (buzón) y posiblemente atributos adicionales para activar sistemas anti-spam o anti-virus.

Como se puede ver este sistema LDAP recibirá cientos de consultas cada día (una por cada email recibido y una cada vez que el usuario se conecta mediante POP3 o webmail). No obstante el número de modificaciones diarias es muy bajo, ya que solo se puede cambiar la contraseña o dar de baja al usuario, operaciones ambas que no se realizan de forma frecuente.

Sistema de autenticación a una red

Cada usuario se identifica por un nombre de usuario y los atributos asignados son la contraseña, los permisos de acceso, los grupos de trabajo a los que pertenece, la fecha de caducidad de la contraseña…

Este sistema recibirá una consulta cada vez que el usuario acceda a la red y una más cada vez que acceda a los recursos del grupo de trabajo (directorios compartidos, impresoras…) para comprobar los permisos del usuario.

Frente a estos cientos de consultas solo unas pocas veces se cambia la contraseña de un usuario o se le incluye en un nuevo grupo de trabajo.

1.5. Diferencias con una base de datos relacional

Las características de una base de datos relacional (RDBMS o Relation Database Management Systems) son:

- **Realizan operaciones de escritura intensivas:** las bases de datos relacionales estás preparadas para hacer un uso constante de operaciones orientadas a transacciones, que implican la modificación o borrado constante de los datos almacenados.
- **Esquema específico** para cada aplicación: las bases de datos relacionales son creadas para cada aplicación específica, siendo complicado adaptar los esquemas a nuevas aplicaciones.
- **Modelo de datos complejo**: permiten manejar complejos modelos de datos que requieren muchas tablas, foreign keys, operaciones de unión (join) complejas…
- **Integridad de datos**: todos sus componentes están desarrollados para mantener la consistencia de la información en todo momento. Esto incluye

operaciones de rollback, integridad referencial y operaciones orientadas a transacciones.
- Además las **transacciones se efectúan siempre aisladas** de otras transacciones. De tal forma que si dos transacciones están ejecutándose de forma concurrente los efectos de la transacción A son invisibles a la transacción B y viceversa, hasta que ambas transacciones han sido completadas.
- Disponen de **operaciones de roll-back** (vuelta atrás). Hasta el final de la transacción ninguna de las acciones llevadas a cabo pasa a un estado final. Si el sistema falla antes de finalizar una transacción todos los cambios realizados son eliminados (roll-back)

Las **características de un servidor LDAP** son:
- **Operaciones de lectura muy rápidas**. Debido a la naturaleza de los datos almacenados en los directorios las lecturas son más comunes que las escrituras.
- **Datos relativamente estáticos**. Los datos almacenados en los directorios no suelen actualizarse con mucha frecuencia.
- **Entorno distribuido**, fácil replicación
- **Estructura jerárquica**. Los directorios almacenan la información de forma jerárquica de forma nativa.
- **Orientadas a objetos**. El directorio representa a elementos y a objetos. Los objetos son creados como entradas, que representan a una colección de atributos.
- **Esquema Standard**. Los directorios utilizan un sistema standard que pueden usar fácilmente diversas aplicaciones.
- **Atributos multi-valor**. Los atributos pueden almacenar un valor único o varios.
- **Replicación multi-master**. Muchos de los servidores LDAP permiten que se realicen escrituras o actualizaciones en múltiples servidores.

1.6. Historia de LDAP

LDAP aparece con el estándar de los directorios de servicios. La versión original fue desarrollada por la Universidad de Michigan. La primera versión no se usó y fue en 1995 cuando se publicaron los RFC (Request For Comments) de la versión LDAPv2. Los RFC para la versión LDAPv3 fueron publicados en 1997. La versión 3 incluía características como las listas de acceso (control access lists) y replicación de directorios. Los RFCs asociados con LDAP son:

RFC1777 - Lightweight Directory Access Protocol. (Obsoletes RFC1487)
RFC1778 - The String Representation of Standard Attribute Syntaxes
RFC1779 - A String Representation of Distinguished Names (Obsoletes

RFC1485)
RFC1823 - The LDAP Application Program Interface
RFC1960 - A String Representation of LDAP Search Filters (Obsoletes RFC1558).
RFC 2251 - Lightweight Directory Access Protocol (v3).
RFC 2252 - LDAPv3 Attribute Syntax Definitions.
RFC 2253 - UTF-8 String Representation of Distinguished Names.
RFC 2254 - The String Representation of LDAP Search Filters.
RFC 2255 - The LDAP URL Format.
RFC 2256 - A Summary of the X.500(96) User Schema for use with LDAPv3..
RFC2829 Authentication Methods for LDAP.
RFC2830 - Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security.
RFCs relacionados.
RFC1274 - The COSINE and Internet X.500 Schema.
RFC1279 - X.500 and Domains.
RFC1308 - Executive Introduction to Directory Services Using the X.500 Protocol.
RFC1309 - Technical Overview of Directory Services Using the X.500 Protocol.
RFC1617 - Naming and Structuring Guidelines for X.500 Directory Pilots (Obsoletes RFC1384).
RFC1684 - Introduction to White Pages services based on X.500.
RFC2079 - Definition of an X.500 Attribute Type and an Object Class to Hold Uniform .

1.7. Servidores LDAP disponibles en el mercado

Los más usados son:

- OpenLDAP – http://www.openldap.org

- Sun SunONE 5.2 – http://www.sun.com/software/products/directory_srvr/home_directory.html
- Siemens DirX Server 6.0 – http://www.siemens.com/directory
- Syntegra Intrastore Server 2000 - http://www.syntegra.com/us/directory_messaging/
- Computer Associates eTrust Directory 3.6 - http://www3.ca.com/Solutions/Product.asp?ID=160
- Novell NDS Corporate Edition 8.7.1 - http://www.novell.com/coolsolutions/nds/
-Microsoft ADS - Windows 2000 server edition - http://www.microsoft.com/windows2000/technologies/directory/ad/default.a...

A continuación se muestra una comparativa en la implementación del servicio Ldap con otras plataformas.

Plataformas	**Open LDAP**	**Sun ONE**	**DirX Server**	**Intrastore**	**eTrust**	**NDS**	**ADS**
K4 (UMich) bind	S	no	?	?	?	N	no
LDAPv2 protocol	S	S	?	?	?	?	?
LDAPv3 protocol	S	S	S	S	S	?	S
K5 bind	S	no	?	?	?	N	S
SASL GSSAPI (Krb5) Auth	S	S	?	?	?	?	S
Scalable > 200K entries	S	S	S	?	S	?	?
Solaris 8	S	S	S	S	S	S	no
Search limit tied to binddn	S	?	?	?	?	?	?
Multi-Master	S	S	?	?	?	?	?
Supports "<text>	N	?	?	?	?	?	?

*(space)<text>" search							
Support avail.	S*	S	S	S	S	S	S

* Se realiza a través de listas de correo, se puede contratar soporte técnico con empresas como Symas Corp., Mind NV, or Inter7.

2. Administración de LDAP

2.1. Introducción a la estructura de árbol

Tradicionalmente se han usado las estructuras de árbol para jerarquizar la información contenida en un medio. El ejemplo más claro es la estructura de carpetas (directorios) de un sistema operativo. Esta organización nos permite ordenar la información en subdirectorios que contienen información muy específica.

Otro ejemplo muy común son los servidores DNS que nos permiten acceder a distintos servicios concretos que representan un dominio, por ejemplo

www.empresa.com – servidor www principal de la empresa
www.admin.empresa.com – servidor de administración
mail.empresa.com – servidor de mail de la empresa
us.mail.empresa.com – servidor secundario de correo en USA
es.mail.empresa.com – servidor secundario de correo en España

2.2. Definición de términos

Entradas

El modelo de información de LDAP está basado en entradas. Una entrada es una colección de atributos que tienen un único y global Nombre Distintivo (DN). El DN se utiliza para referirse a una entrada sin ambigüedades. Cada atributo de una entrada posee un tipo y uno o más valores. Los tipos son normalmente palabras nemotécnicas, como “cn” para common name, o “mail” para una dirección de correo.

La sintaxis de los atributos depende del tipo de atributo. Por ejemplo, un atributo cn puede contener el valor “Jose Manuel Suarez”. Un atributo email

puede contener un valor “jmsuarez@ejemplo.com”. El atributo jpegPhoto ha de contener una fotografía en formato JPEG.

Atributos

Los datos del directorio se representan mediante pares de atributo y su valor. Por ejemplo el atributo commonName, o cn (nombre de pila), se usa para almacenar el nombre de una persona. Puede representarse en el directorio a una persona llamada José Suarez mediante:

• cn: José Suarez

Cada persona que se introduzca en el directorio se define mediante la colección de atributos que hay en la clase de objetos person.

Otros atributos:

• givenname: José
• surname: Suarez
• mail: jmsuarez@ejemplo.com

Los atributos requeridos son aquellos que deben estar presentes en las entradas que utilicen en la clase de objetos. Todas las entradas precisas de los atributos permitidos son aquellos que pueden estar presentes en las entradas que utilicen la clase de objetos.

Por ejemplo, en la clase de objetos person, se requieren los atributos cn y sn. Los atributos description (descripción), telephoneNumber (número de teléfono), seealso (véase también), y userpassword (contraseña del usuario) se permiten pero no son obligatorios.

Cada atributo tiene la definición de sintaxis que le corresponde. La definición de sintaxis describe el tipo de información que proporciona ese atributo:

1. Bin binario
2. ces cadena con mayúsculas y minúsculas exactas (las mayúsculas y minúsculas son significativas durante las comparaciones)
3. cis cadena con mayúsculas y minúsculas ignoradas (las mayúsculas y minúsculas no son significativas durante las comparaciones)
4. tel cadena de número de teléfono (como cis, pero durante las comparaciones se ignoran los espacios en blanco y los guiones"_")
5. dn "distinguished name" (nombre distintivo)

Tipos de Atributos

Una definición de tipo de atributo especifica la sintaxis de un atributo y cómo se ordenan y comparan los atributos de ese tipo.

Los tipos de atributos en el directorio forman un árbol de clases. Por ejemplo, el tipo de atributo "commonName" es una subclase del tipo de atributo "name".

Hay atributos obligatorios y opcionales listados en la siguiente tabla:

Identificador de Atributo Descripción del Valor de Atributo
NUMERICOID (obligatorio) Identificador de Objeto Único (OID)
NAME Nombre del Atributo
DESC Descripción del Atributo
OBSOLETE "true" si es obsoleto; "false" o ausente si no lo es
SUP Nombre del tipo de atributo superior del que se deriva el tipo de atributo
EQUALITY Nombre ó OID de la regla de correspondencia si la igualdad de correspondencia está permitida; ausente si no lo está
ORDERING Nombre o OID de la regla de correspondencia si está permitida la ordenación; ausente si no lo está.
SUBSTRING Nombre o OID de la regla de correspondencia si está permitida la correspondencia de sub-string ausente si no lo está.
SYNTAX OID numérico de la sintaxis de los valores de este tipo
SINGLE-VALUE "true" si el atributo no es multi-valor; "false" o ausente si lo es
COLLECTIVE "true" si el atributo es colectivo; "false" o ausente si no lo es
NO-USER-MODIFICATION "true" si el atributo no es modificable por el usuario; "false" o ausente si lo es
USAGE Descripción del uso del atributo
Estos atributos corresponden a la definición de "AttributeTypeDescription" en la RFC 2252.

LDIF

Para importar y exportar información de directorio entre servidores de directorios basados en LDAP, o para describir una serie de cambios que han de aplicarse al directorio, se usa en general el fichero de formato conocido como LDIF (formato de intercambio de LDAP).

Un fichero LDIF almacena información en jerarquías de entradas orientadas a objeto. Todos los servidores LDAP que incluyen una utilidad para convertir ficheros LDIF a formato orientadas a objeto. Normalmente es un fichero ASCII.

EJEMPLO:
Un fichero LDIF corriente tiene este aspecto:

dn: uid=jmsuarez,ou=People,dc=empresa,dc=com
uid: jmsuarez
cn: Jose Manuel Suarez
objectclass: account
objectclass: posixAccount
objectclass: top
loginshell: /bin/bash
uidnumber: 512
gidnumber: 300
homedirectory: /home/jmsuarez
gecos: Jose Manuel Suarez,,,,
userpassword: {crypt}LPnaOoUYN57Netaac

Como se puede notar, cada entrada está identificada por un nombre distintivo: DN ("distinguished name", nombre distintivo) está compuesto por el nombre de la entrada en cuestión, más la ruta de nombres que permiten rastrear la entrada hacia atrás hasta la parte superior de la jerarquía del directorio.

Objetos

En LDAP, una clase de objetos define la colección de atributos que pueden usarse para definir una entrada. El estándar LDAP proporciona estos tipos básicos para las clases de objetos:

1. Grupos en el directorio, entre ellos listas no ordenadas de objetos individuales o de grupos de objetos.
2. Emplazamientos, como por ejemplo el nombre del país y su descripción.
3. Organizaciones que están en el directorio.
4. Personas que están en el directorio.

Una entrada determinada puede pertenecer a más de una clase de objetos. Por ejemplo, la entrada para personas se define mediante la clase de objetos person, pero también puede definirse mediante atributos en las clases de objetos inetOrgPerson, groupOfNames y organization. La estructura de clases

de objetos del servidor determina la lista total de atributos requeridos y permitidos para una entrada concreta.

2.3. Integración de LDAP con otros sistemas

Una vez que hayamos configurado e instalado LDAP lo podemos usar como repositorio de datos para multitud de aplicaciones que disponen de soporte

- Radius
- Samba
- DNS
- Mail Transfer Agents
- Libretas de direcciones
- Servidores FTP
- Servidores de certificados de seguridad

3. Presentación de OpenLDAP

3.1. Presentación de OpenLDAP

El proyecto OpenLDAP nació como la continuación de la versión 3.3 del servidor LDAP de la Universidad de Michigan cuando dejaron de desarrollarlo.
OpenLDAP es un servidor LDAP que se distribuye bajo licencia GNU (OpenSource), que permite que el software se pueda usar de forma gratuita tanto de forma educativa como profesional. Además disponemos del código fuente para poder realizar nuestras propias modificaciones.
Se puede descargar de forma gratuita en la siguiente dirección
http://www.openldap.org/software/download/

A la hora de descargarte OpenLDAP verás que hay varias versiones disponibles:

- OpenLDAP Release. Las últimas versiones de OpenLDAP para uso general. OpenLDAP-2.2.15 es la última versión disponible.
- OpenLDAP Stable Release. Es la última versión que ha sido intensamente probada y suele ser la más fiable de las versiones disponibles.
- OpenLDAP Test Releases. Ocasionalmente los programadores de OpenLDAP hacen disponible una versión beta o gamma. Estas versiones son sólo para pruebas y no son para uso general.

En este momento OpenLDAP-2.2.13, es la versión considerada más estable.
Las versiones OpenLDAP 2.x funcionan con la versión 3 de LDAP (RFC 3377).
LDAPv3 es es standar actual para todos los servidores LDAP.
Los paquetes que incluyen las distribuciones de OpenLDAP son:

• servidor LDAP (slapd)
• servidor de replicación LDAP (slurpd)
• Software Development Kit (ldap)
• Utilidades, herramientas, ejemplos…

Toda la documentación sobre el producto puede consultarse en
http://www.openldap.org/doc/

El coordinador del proyecto OpenLDAP se llama **Kurt D. Zeilenga** y es fácil contactar con él a través de las listas de correo.
Además de desarrollar OpenLDAP Kurt trabaja en IBM donde es Ingeniero de investigación de Servicios de Directorio y desarrollador de IBM Linux Technology Center.

3.2. Requisitos para instalar OpenLDAP

Sistema operativo. OpenLDAP funciona en los siguientes sistemas operativos:
Apple Mac OS X
Linux: Debian, RedHat, Suse, Fedora, Mandrake…
FreeBSD
IBM AIX
Microsoft Windows 2000/NT
NetBSD
Solaris

4. Administración de OPENLDAP

4.1. Cálculo del dimensionamiento del servidor/servidores

Elige bien tu plataforma hardware:

- **Procesador:** Normalmente servidores multiporcesador.
- **Discos duros:** Para OpenLDAP los más óptimo es que uses un disco duro para el sistema operativo (preferiblemente en RAID) y un disco separado para la base de datos (normalmente sin RAID). Elige discos duros muy rápidos, esta es la optimización más importante para OpenLDAP.
- **Tamaño de la memoria:** Dependerá del número de entradas que quieras almacenar y del número de atributos que use cada entrada. También de las pruebas de carga que realices y sus resultados. Normalmente necesitarás entre 1 GB y 4 GB.
- **Instalación del sistema operativo**
- Elegir una instalación simple, sólo con los complementos imprescindibles.

- Actualizar el sistema operativo con los últimos parches o service packs (ej.: sunsolve.sun.com, redhat.com, windowsupdate.microsoft.com.…)
- Elegir un sistema de archivos adecuado, normalmente: Ext3 para Linux o UFS con LOGGING para Solaris.
- Parar todos los servicios y demonios que no se vayan a usar.
- Securizar el servidor.
- Optimizar los parámetros del sistema operativo (hay diversos métodos de hacerlo que no se incluyen en este manual)
- Optimizar la configuración de la pila TCP.

4.2. Nomenclatura

Antes de instalar el servidor elige una nomenclatura de directorios para todos tus trabajos (debes pensar siempre en las actualizaciones posteriores a la instalación actual)
Un ejemplo es usar un directorio como /opt/apps
/opt/source/openldap-2.1.25 directorio con el código fuente

/opt/apps/openldap-2.1.25 directorio para tu aplicación

/opt/apps/openldap es un link a la aplicación

/opt/data/openldap es el directorio para la base de datos

/opt/backup es el backup diario

Con una nomenclatura como esta es muy fácil implementar actualizaciones de la aplicación.Elige además una nomenclatura para todos los objetos, atributos, usuarios.

4.3. Descarga del software

Es preferible descargar y compilar OpenLDAP frente a instalarlo desde un paquete (RPM, deb o similar), porque estos paquetes no suelen venir muy optimizados.
Descarga la última versión estable de OpenLDAP (en este momento la 2.2.15) desde http://www.openldap.org/.Verifica la firma MD5 del paquete que te has descargado usando el siguiente comando:
[root@dep tmp]# md5sum openldap-2.2.15.tgz
Ahora verifica que la firma es exactamente la misma que la contenida en un archivo llamado openldap-2.2.15.md5 que te puedes descargar desde el servidor FTP de OpenLDAP.
Desconfía de servidores FTP que no sean los oficiales y de paquetes cuya firma MD5 no coincida con los de las páginas oficiales de OpenLDAP.

4.4. Compilación e instalación

Sitúate en el directorio donde hayas descomprimido el código fuente y ejecuta los comandos:

./configure
make
make depend
su make install

Conseguiremos que nuestro software esté mucho más optimizado si desactivamos antes de compilar las opciones que no vamos a usar y activamos otras específicas, por ejemplo:

**./configure **
**--disable-debug **
**--disable-ipv6 **
**--enable-crypt **
**--without-tls **
--with-threads

Esto le prepara a OpenLDAP para configurarse de una forma especial:
- Sin soporte para debugging.
- Sin soporte para IPv6.
- Activa el soporte para passwords cifrados (con crypt).
- Desactiva la encriptación TLS/SSL.
- Activa el soporte para threads.

5. CONFIGURAR LDAP USANDO YAST

Introducción

El problema de la Administración de Identidades

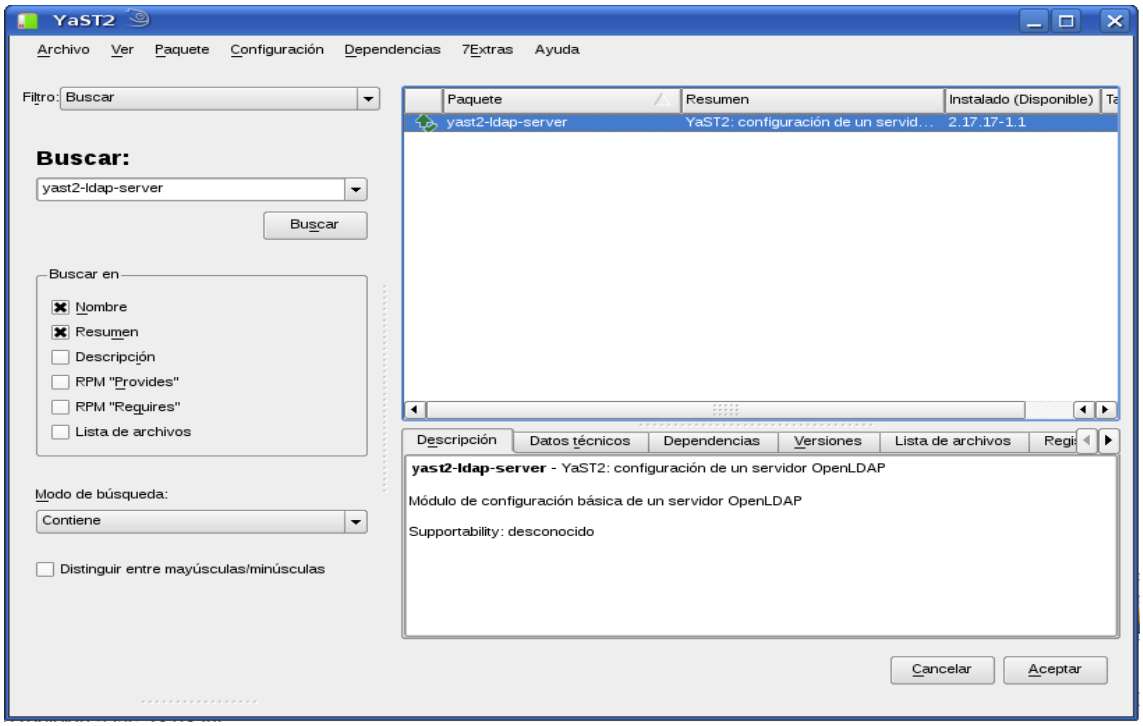
- Cada Usuario tiene múltiples identidades en la empresa
- Múltiples administradores para cada usuario
- No existe un método seguro para compartir las identidades de usuarios entre ambientes linux, UNIX® y Windows®
- No existe un único punto de administración para cada usuario

Costos en Seguridad y Mesa de Ayuda

- Un usuario promedio utiliza 5+ claves
- 55% de los usuarios escribe la clave en papel al menos una vez
- 9% de todos los usuarios escriben en papel todas las claves
- 51% de todos los usuarios requieren ayuda de TI porque olvidaron su clave
- 25% de todas las consultas a las mesas de ayuda están relacionadas con claves

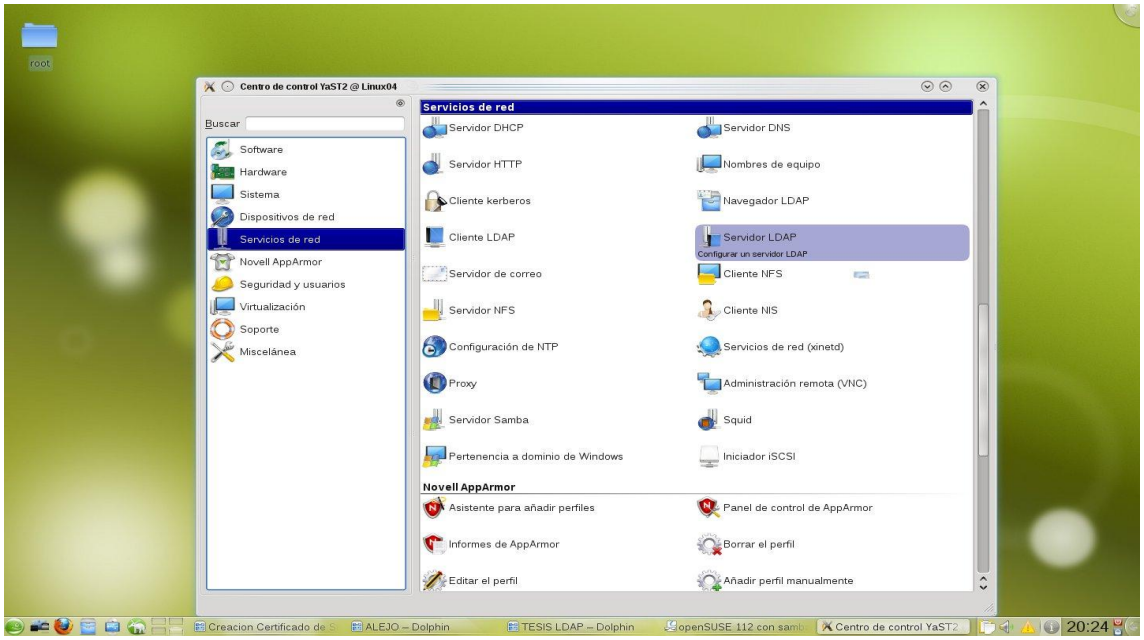
5.2 Software necesario / Instalacion

- Inicie yast / Software / Instalar-desinstalar software y adicione el paquete yast2-ldap-server, damos click en aceptar.

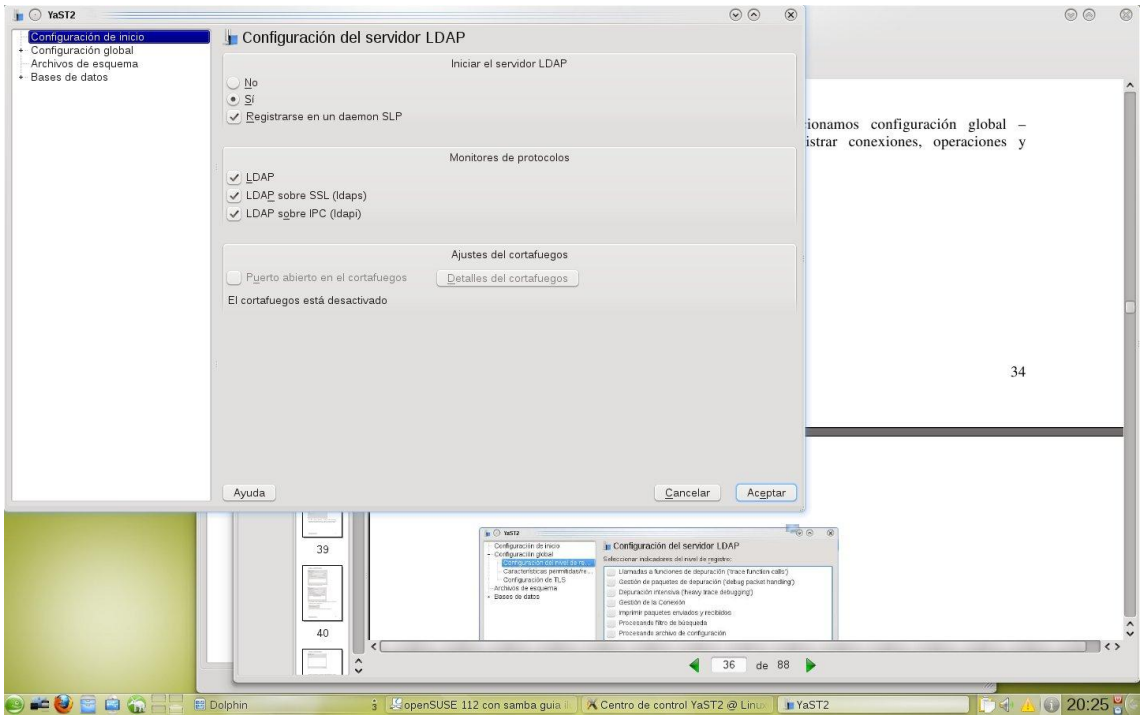


5.3 Configuración

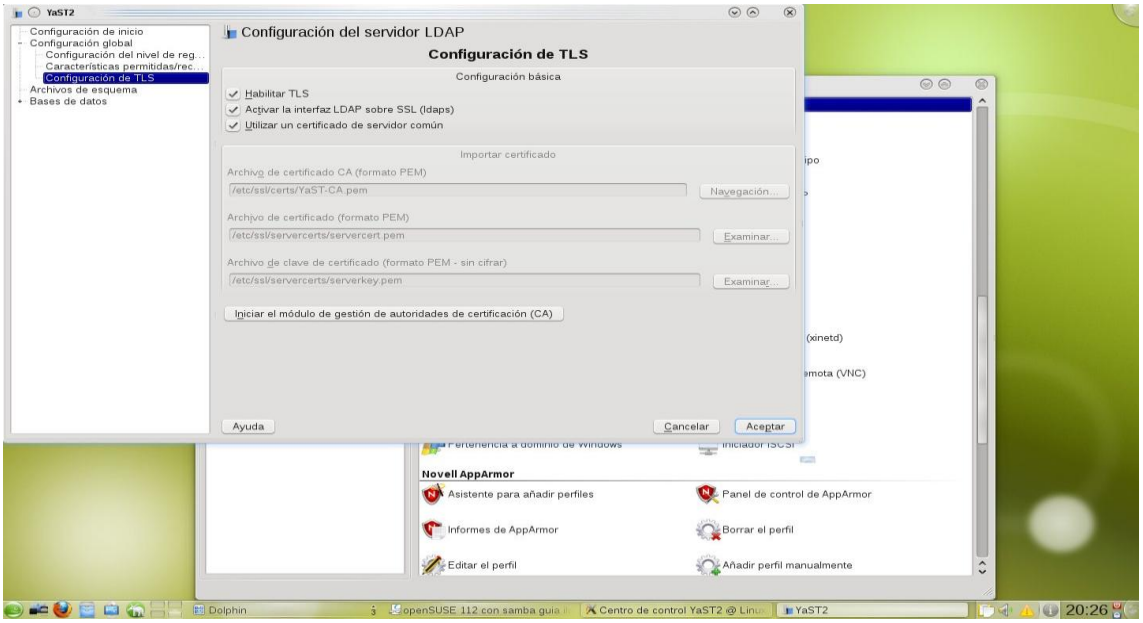
- Luego de realizada la instalación, iniciamos YaST nos ubicamos en Servicios de red y damos click a Servidor LDAP



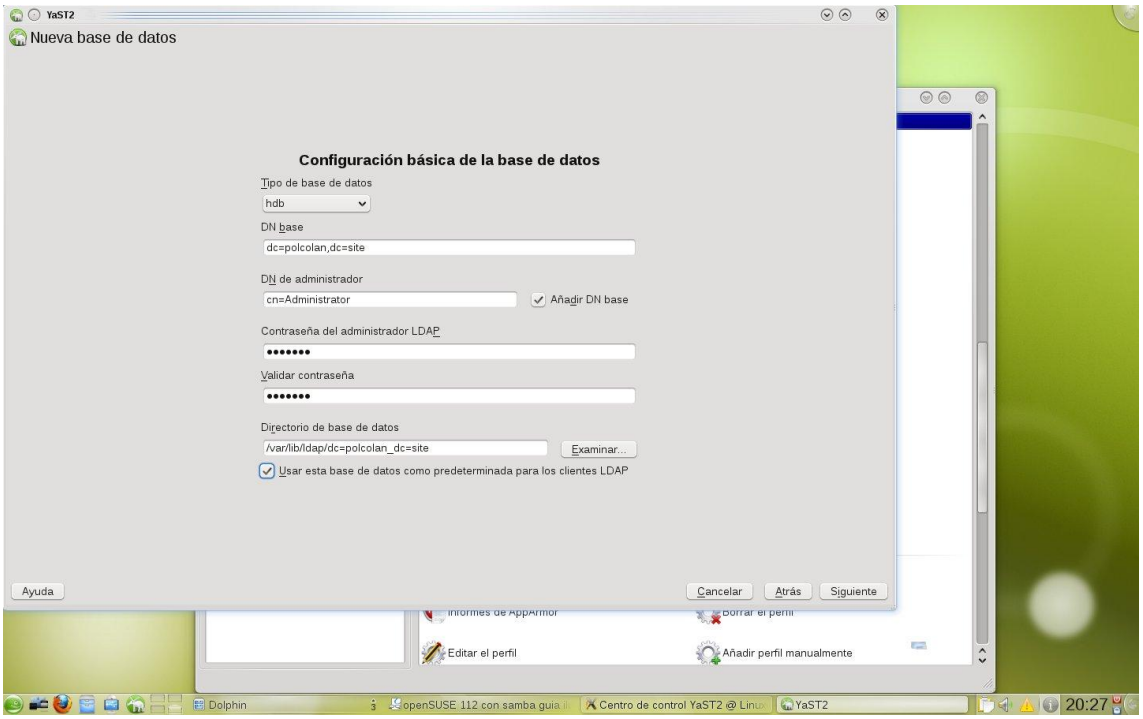
- Vamos a configuración de inicio, activamos las siguientes características en iniciar el servidor LDAP damos click en Si y Registrarse en un daemon SLP, luego activamos todas las opciones del área Monitores de protocolos.



- Damos click en configuración global y seleccionamos Configuración de TLS, activamos las tres opciones que nos aparecen en Configuración Básica.

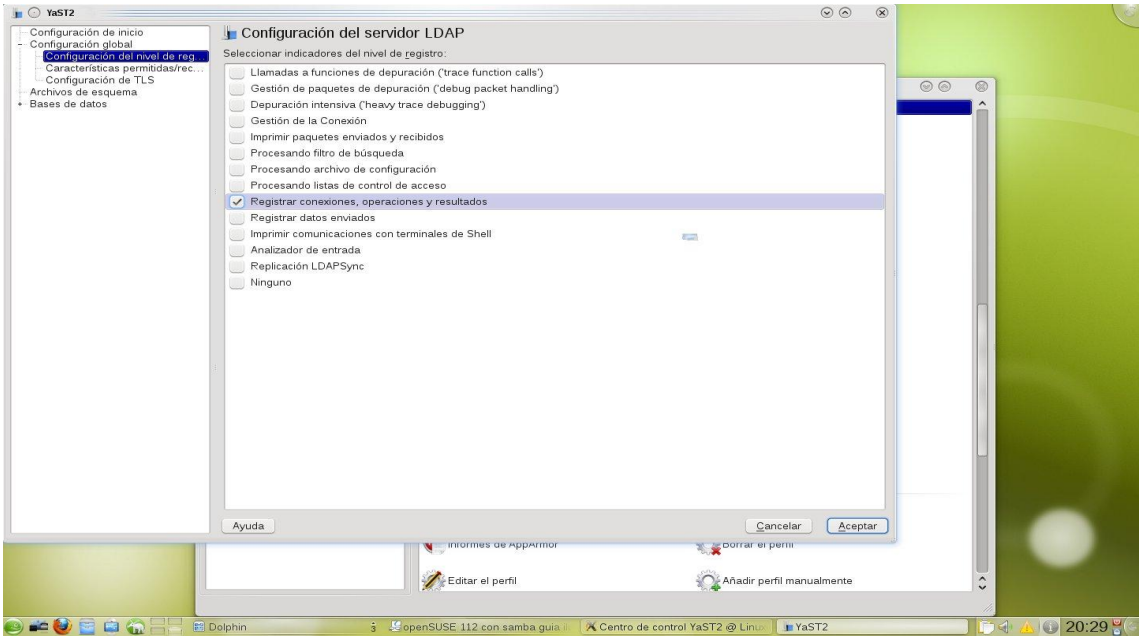


- Nuestro siguiente paso es dar click en Bases de datos y creamos una nueva base de datos, nuestro DN base será el nombre de nuestro dominio, y el DN de administrador será nuestro administrador de la base de datos, digitamos una contraseña para el administrador y activamos la opción Usar esta base de datos como predeterminada para los clientes LDAP, damos click en siguiente.

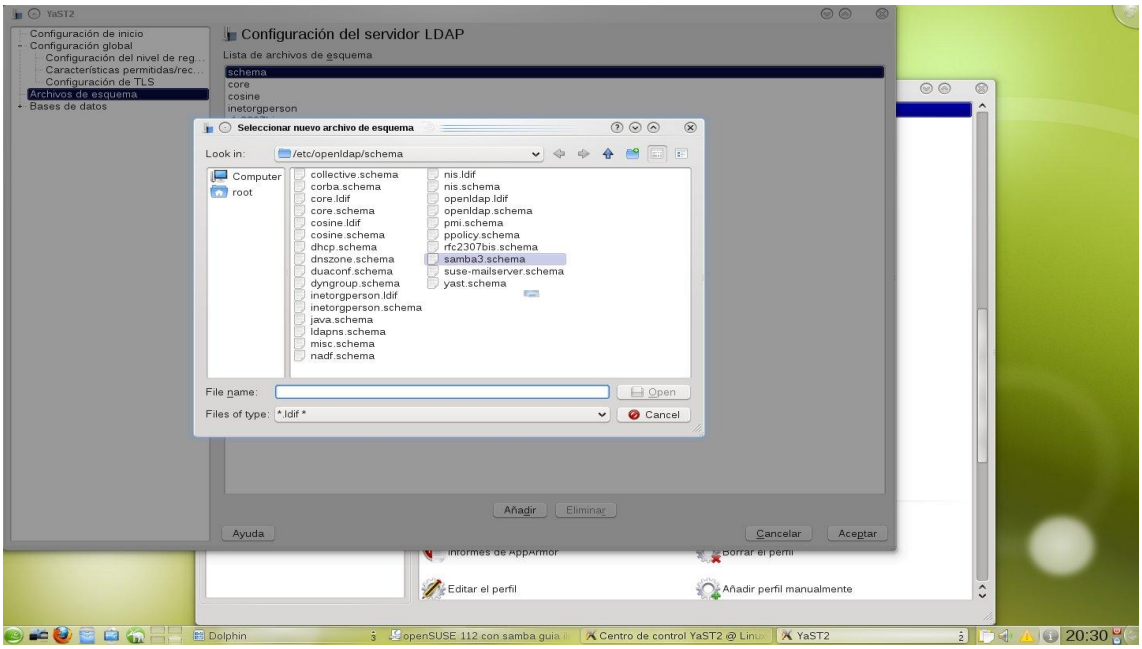


- Luego de realizar la configuración de nuestra base de datos, volvemos a la configuración global / opción Configuración del nivel de registro y activamos

la característica Registrar conexiones, operaciones y resultados como se muestra a continuación.



- Luego de realizar la configuración del nivel de registro, hacemos click en Archivos de esquema, damos click en el botón añadir y seleccionamos el archivo samba3.schema.



Damos click en aceptar y ha quedado configurado nuestro servidor LDAP.

6. GESTIÓN DE DATOS EN EL DIRECTORIO LDAP

OpenLDAP ofrece una serie de herramientas para la administración de datos en el directorio LDAP. Las cuatro herramientas más importantes para añadir, suprimir, buscar y modificar los datos almacenados se explican brevemente a continuación.

6.1. Inserción de datos en un directorio LDAP

Una vez que la configuración del servidor LDAP en /etc/openldap/lsapd.conf sea correcta y esté lista (presenta las entradas apropiadas para suffix, directory, rootdn, rootpw e index), siga con la introducción de registros. OpenLDAP cuenta con el comando **ldapadd** para esta tarea. Si es posible, añada los objetos a la base de datos en paquetes por razones prácticas. LDAP es capaz de procesar el formato LDIF (formato de intercambio de datos de LDAP) para esto. Un archivo LDIF es un archivo de texto que puede contener un número arbitrario de pares de atributo y valor. Consulte los archivos de esquema declarados en slapd.conf para las clases y atributos de objetos disponibles.

6.1.1. Estructura de un archivo LDIF

The SUSE Organization

dn: dc=suse,dc=de

objectClass: dcObject

objectClass: organization

o: SUSE AG dc: suse

The organizational unit development (devel)

dn: ou=devel,dc=suse,dc=de

objectClass: organizationalUnit

ou: devel

The organizational unit documentation (doc)

dn: ou=doc,dc=suse,dc=de

objectClass: organizationalUnit

ou: doc

The organizational unit internal IT (it)

dn: ou=it,dc=suse,dc=de

objectClass: organizationalUnit

ou: it

6.1.2. Codificación de archivos LDIF

LDAP funciona con UTF-8 (Unicode). Las diéresis deben codificarse correctamente. Utilice un editor que sea compatible con UTF-8, como Kate o versiones recientes de Emacs. De lo contrario, evite las diéresis y otro tipo de caracteres especiales o use **recode** para volver a codificar la entrada en UTF-8. Guarde el archivo con el sufijo .ldif y, a continuación, trasládelo al servidor con este comando:

ldapadd -x -D <dn del administrador> -W -f <archivo>.ldif

-x desconecta la autenticación con SASL en este caso. -D indica el usuario que llama a la operación.

El DN válido del administrador se introduce tal y como se ha configurado en slapd.conf. En el ejemplo actual, es cn=admin,dc=suse,dc=de. -W evita tener que introducir la contraseña en la línea de comando (en texto no cifrado) y activa un indicador de contraseña aparte.

Esta contraseña se ha determinado previamente en slapd.conf con rootpw. -f traslada el nombre del archivo.

ldapadd con ejemplo.ldif

ldapadd -x -D cn=admin,dc=suse,dc=de -W -f ejemplo.ldif

Enter LDAP password:

adding new entry "dc=suse,dc=de"

adding new entry "ou=devel,dc=suse,dc=de"

adding new entry "ou=doc,dc=suse,dc=de"

adding new entry "ou=it,dc=suse,dc=de"

Los datos de usuario de los usuarios se pueden preparar en archivos LDIF independientes.

Datos de LDIF para Tux

coworker Tux

dn: cn=Tux Linux,ou=devel,dc=suse,dc=de

objectClass: inetOrgPerson

cn: Tux Linux

givenName: Tux

sn: Linux

mail: tux@suse.de

uid: tux

telephoneNumber: +49 1234 567-8

Los archivos LDIF pueden contener un número arbitrario de objetos. Es posible enviar ramas completas al servidor de una vez o sólo partes, tal y como se muestra en el ejemplo de los objetos individuales. Si es necesario modificar algunos datos con más frecuencia, se recomienda realizar una pequeña subdivisión de los objetos individuales.

6.1.3. Modificación de datos en el directorio LDAP

La herramienta **ldapmodify** sirve para modificar los datos almacenados. La manera más sencilla de hacerlo es modificar el archivo LDIF y, seguidamente, mandar el archivo modificado al servidor LDAP. Para cambiar el número de teléfono del usuario Tux de +49 1234 567-8 a +49 1234 567-10, edite el archivo LDIF como se muestra acontinuacion:

Archivo LDIF modificado tux.ldif

coworker Tux

dn: cn=Tux Linux,ou=devel,dc=suse,dc=de

changetype: modify

replace: telephoneNumber

telephoneNumber: +49 1234 567-10

Importe el archivo modificado al directorio LDAP con el siguiente comando:

ldapmodify -x -D cn=admin,dc=suse,dc=de -W -f tux.ldif

De manera alternativa, envíe los atributos que va a cambiar directamente a **ldapmodify**. Este procedimiento se describe a continuación:

1. Inicie **ldapmodify** e introduzca la contraseña:
2. ldapmodify -x -D cn=admin,dc=suse,dc=de -W
3. Enter LDAP password:
4. Introduzca los cambios con cuidado teniendo en cuenta el orden de la sintaxis que se describe a continuación:
5. dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
6. changetype: modify
7. replace: telephoneNumber
   telephoneNumber: +49 1234 567-10

6.1.4. Búsqueda o lectura de datos desde un directorio LDAP

OpenLDAP ofrece, mediante el comando **ldapsearch**, una herramienta de línea de comando para buscar datos en un directorio LDAP y leer datos de él. Una consulta sencilla tendría la sintaxis siguiente:

ldapsearch -x -b dc=suse,dc=de "(objectClass=*)"

La opción -b determina la base de la búsqueda (la sección del árbol en la que debe realizarse la búsqueda). En el caso actual, es dc=suse,dc=de. Para realizar una búsqueda más precisa en subsecciones concretas del directorio LDAP (por ejemplo, sólo dentro del departamento devel), pase esta sección a **ldapsearch** con -b. -x pide la activación de la autenticación simple. (objectClass=*) declara que deben leerse todos los objetos contenidos en el directorio.

Esta opción de comando puede usarse tras la creación de un árbol de directorios nuevo para comprobar que se han registrado todas las entradas

correctamente y que el servidor responde tal y como se desea. Puede encontrar más información sobre el uso de **ldapsearch** en la página Man correspondiente (ldapsearch(1)).

6.1.5. Supresión de datos de un directorio LDAP

Suprima las entradas no deseadas con **ldapdelete**. La sintaxis es similar a la de los comandos descritos anteriormente. Para suprimir, por ejemplo, la entrada completa de Tux Linux, emita el siguiente comando:

ldapdelete -x -D cn=admin,dc=suse,dc=de -W cn=Tux \

Linux,ou=devel,dc=suse,dc=de

6.2. El cliente LDAP de YaST

YaST incluye un módulo para configurar la gestión de usuarios basada en LDAP. Si no ha habilitado esta función durante la instalación, inicie el módulo seleccionando 'Servicios de red'+'Cliente LDAP.' YaST habilitará automáticamente cualquier cambio relacionado con PAM y NSS que necesite LDAP (tal y como se describe a continuación) e instalará los archivos necesarios.

6.2.1. Procedimiento estándar

El conocimiento previo de los procesos que actúan en segundo plano de un equipo cliente le ayudará a entender cómo funciona el módulo del cliente LDAP de YaST. Si se activa LDAP para la autenticación de red o se llama al módulo YaST, se instalan los paquetes pam_ldap y nss_ldap y se adaptan los dos archivos de configuración correspondientes. pam_ldap es el módulo PAM responsable de la negociación entre los procesos de inicio de sesión y el directorio LDAP como origen de los datos de autenticación.

pam_unix2.conf adaptado a LDAP

auth: use_ldap
account: use_ldap
password: use_ldap
session: none

Al configurar manualmente los servicios adicionales para usar LDAP, incluya el módulo PAM de LDAP en el archivo de configuración PAM correspondiente al servicio en /etc/pam.d. Los archivos de configuración ya adaptados a los servicios individuales se pueden encontrar en /usr/share/doc/packages/pam_ldap/pam.d/. Copie los archivos adecuados en /etc/pam.d.
La resolución de nombres de glibc mediante el mecanismo nsswitch se adapta al empleo de LDAP con nss_ldap. Se crea un archivo nsswitch.conf nuevo y adaptado en /etc/ con la instalación de este paquete. Las líneas siguientes deben estar presentes en nsswitch.conf para la administración y autenticación del usuario con LDAP.

Adaptaciones en nsswitch.conf
passwd: compat
group: compat
passwd_compat: ldap
group_compat: ldap

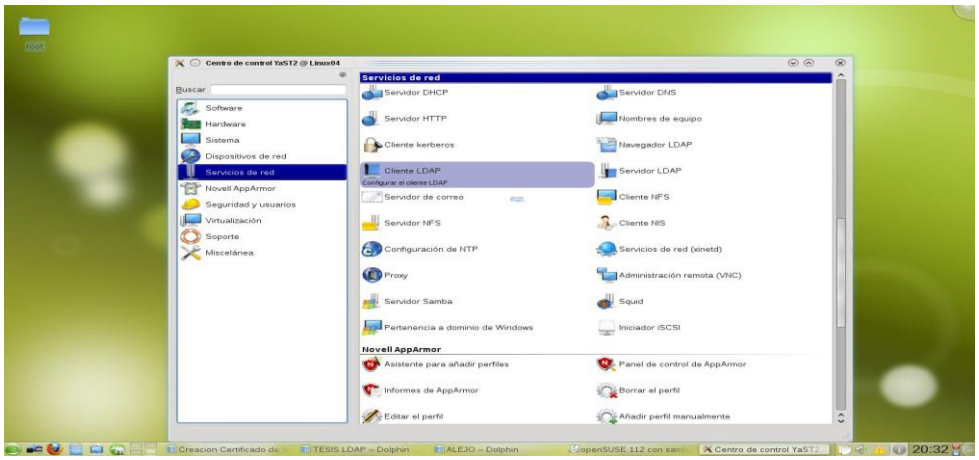
Estas líneas ordenan la biblioteca Resolver de glibc primero para evaluar los archivos correspondientes en /etc y después para acceder al servidor LDAP como orígenes para los datos de autenticación y de usuarios. Compruebe este mecanismo, por ejemplo, leyendo el contenido de la base de datos del usuario con el comando **getent passwd**. El conjunto devuelto debe contener un informe de los usuarios locales del sistema además de todos los usuarios almacenados en el servidor LDAP.
Para impedir que usuarios normales gestionados mediante LDAP puedan iniciar sesión en el servidor con **ssh** o **login**, los archivos /etc/passwd y /etc/group deben incluir una línea adicional. Esta es la línea +::::::/sbin/nologin en /etc/passwd y +::: en /etc/group.

6.2.2. configuración del cliente LDAP

Después de que YaST se haya encargardo de los ajustes iniciales de nss_ldap, pam_ldap, /etc/passwd y /etc/group, podrá conectar sencillamente el cliente con el servidor y dejar que YaST se encargue de la gestión de usuarios mediante LDAP.
Utilice el cliente LDAP de YaST para seguir configurando los módulos de configuración de usuarios y grupos de YaST. Esto incluye la manipulación de los ajustes por defecto para los nuevos grupos y usuarios y el número y la naturaleza de los atributos asignados a un usuario o a un grupo. La gestión de usuarios de LDAP le permite asignar más atributos y diferentes a los usuarios y grupos que las soluciones de gestión de usuarios o grupos tradicionales.

6.2.2.1. Configuración básica

El cuadro de diálogo de configuración básica del cliente LDAP se abre durante la instalación si elige la gestión de usuarios de LDAP o cuando selecciona 'Servicios de red'+'Cliente LDAP' en el Centro de control de YaST en el sistema instalado.

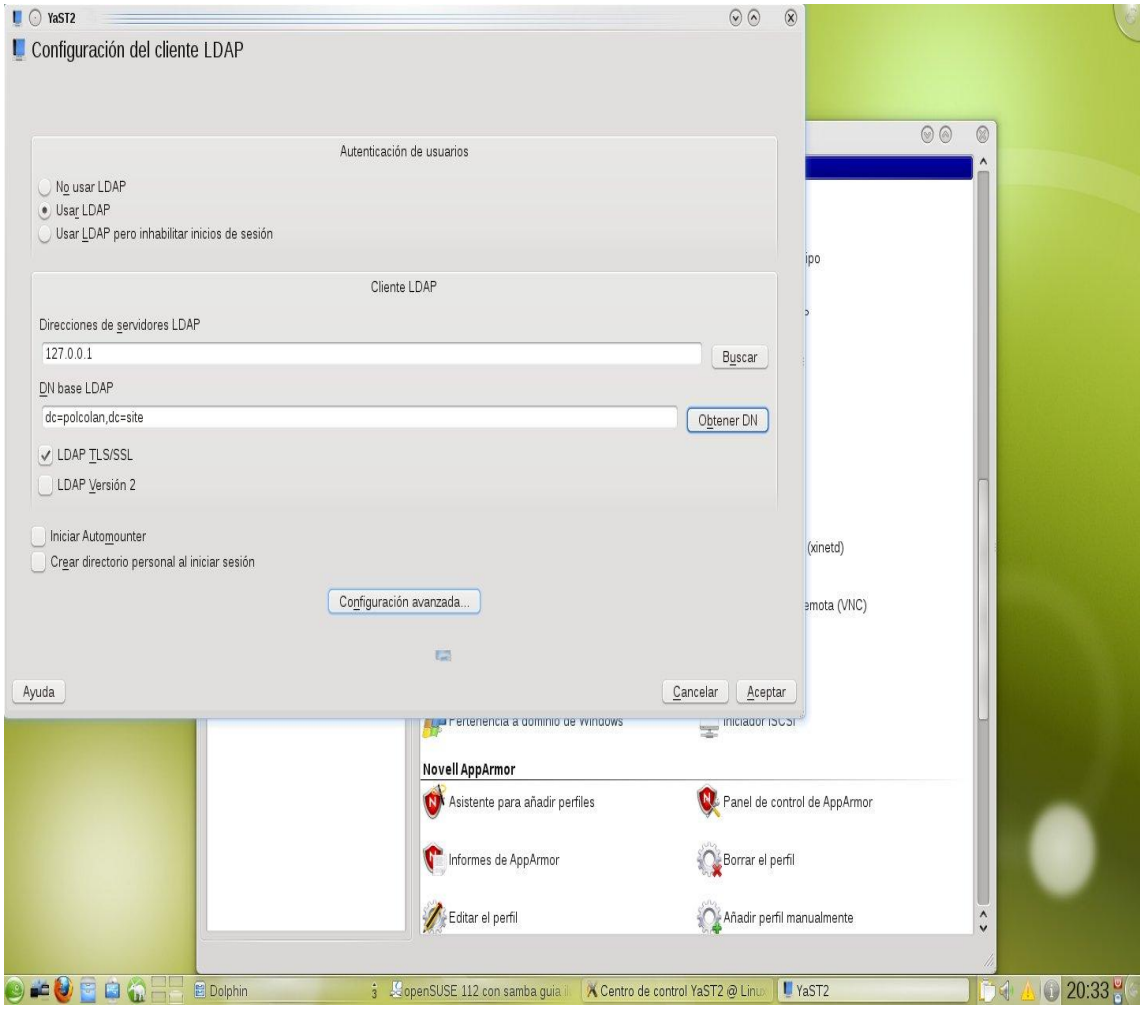


Para autenticar a los usuarios en el equipo con un servidor OpenLDAP y habilitar la gestión de usuarios mediante OpenLDAP, actúe de la siguiente manera:

Haga clic en 'Usar LDAP' para habilitar la utilización de LDAP, luego introduzca la dirección IP del servidor LDAP que va a usar y de click en obtener DN para seleccionar la base de búsqueda en el servidor LDAP.

Si es necesario que la comunicación de TLS o SSL con el servidor esté protegida, seleccione 'LDAP TLS/SSL.'

Si el servidor LDAP sigue usando LDAPv2, habilite explícitamente el uso de esta versión del protocolo seleccionando 'LDAP versión 2.'



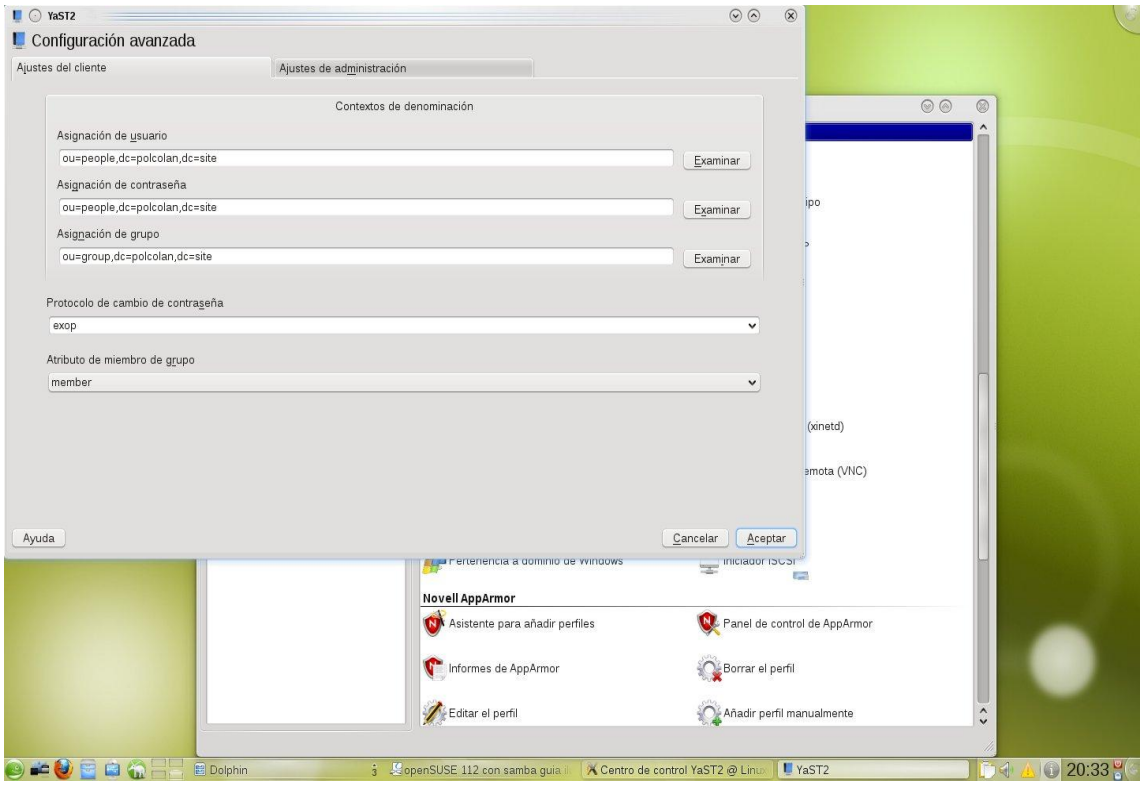
Haga clic en configuración avanzada para realizar otros ajustes.

Para modificar los datos del servidor como administrador, haga clic en Configuración avanzada. El siguiente cuadro de diálogo está dividido en dos pestañas.

En la pestaña Ajustes del cliente, defina los ajustes siguientes según sus necesidades:

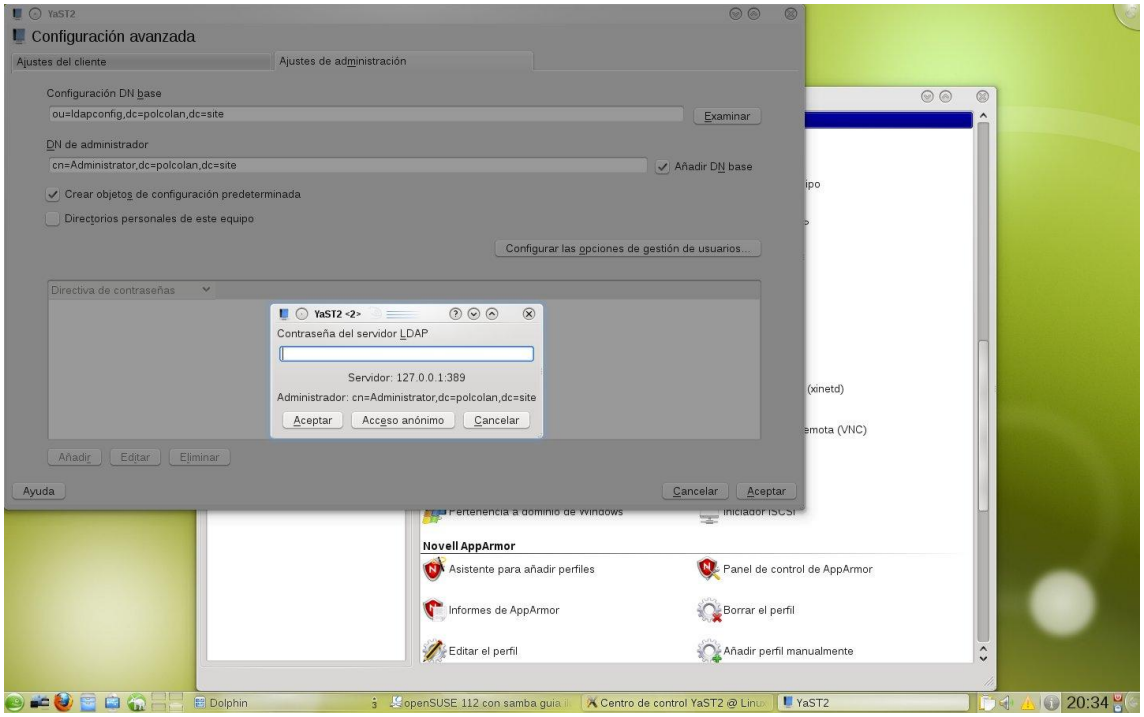
- Si la base de la búsqueda de usuarios, contraseñas y grupos difiere de la base de búsqueda global especificada en DN base de LDAP, introduzca los distintos contextos de denominación en Asignación de usuario, Asignación de contraseña y Asignación de grupo.
- Especifique el protocolo de cambio de contraseña. El método estándar empleado siempre que se cambia una contraseña es el cifrado, lo que quiere decir que los algoritmos hash generados por **crypt** serán los que se

usen. Especifique el grupo LDAP que se va a usar con Atributo de miembros del grupo. El valor por defecto de esta opción es member.



En Ajustes de administración defina los siguientes ajustes:

1. Defina la base para el almacenamiento de los datos de gestión de usuarios mediante Configuración de DN base.
2. Introduzca el valor adecuado para Administrador DN. Este DN debe ser idéntico al valor de rootdn especificado en /etc/openldap/slapd.conf para habilitar a este usuario en concreto de modo que pueda manipular los datos almacenados en el servidor LDAP.
3. Marque Crear objetos de configuración predeterminada para crear los objetos de configuración básicos en el servidor para habilitar la gestión de usuarios mediante LDAP.
4. Si el equipo cliente debe actuar como servidor de archivos para directorios personales por la red, marque Directorios personales de este equipo.

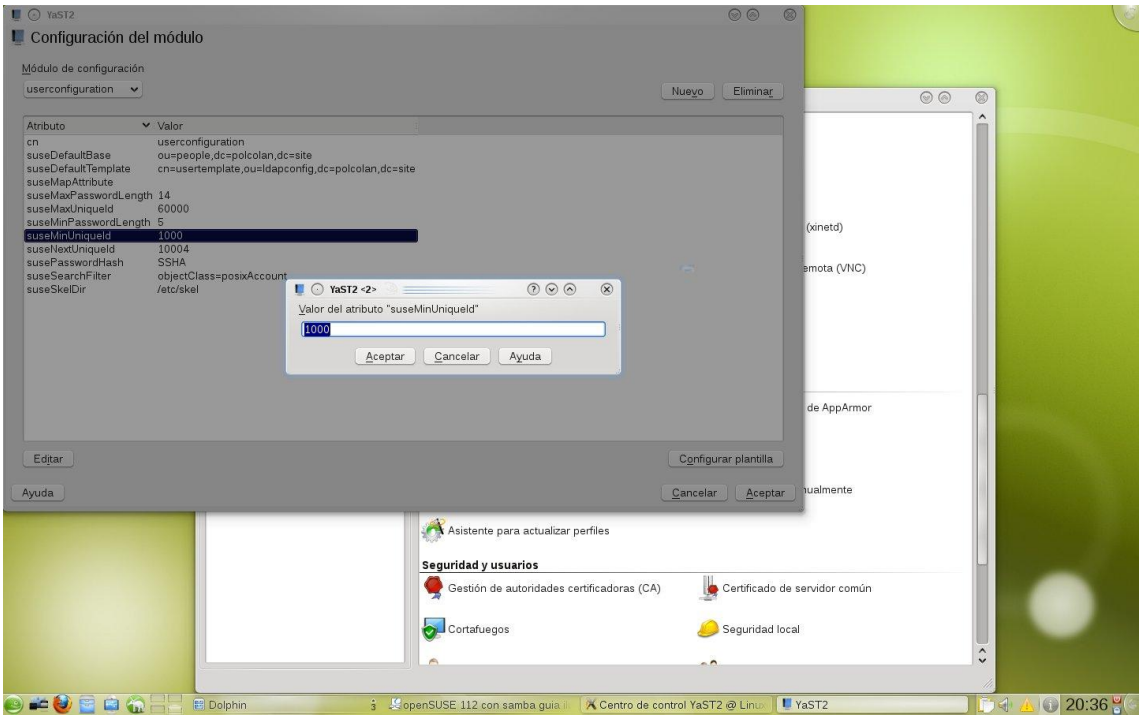


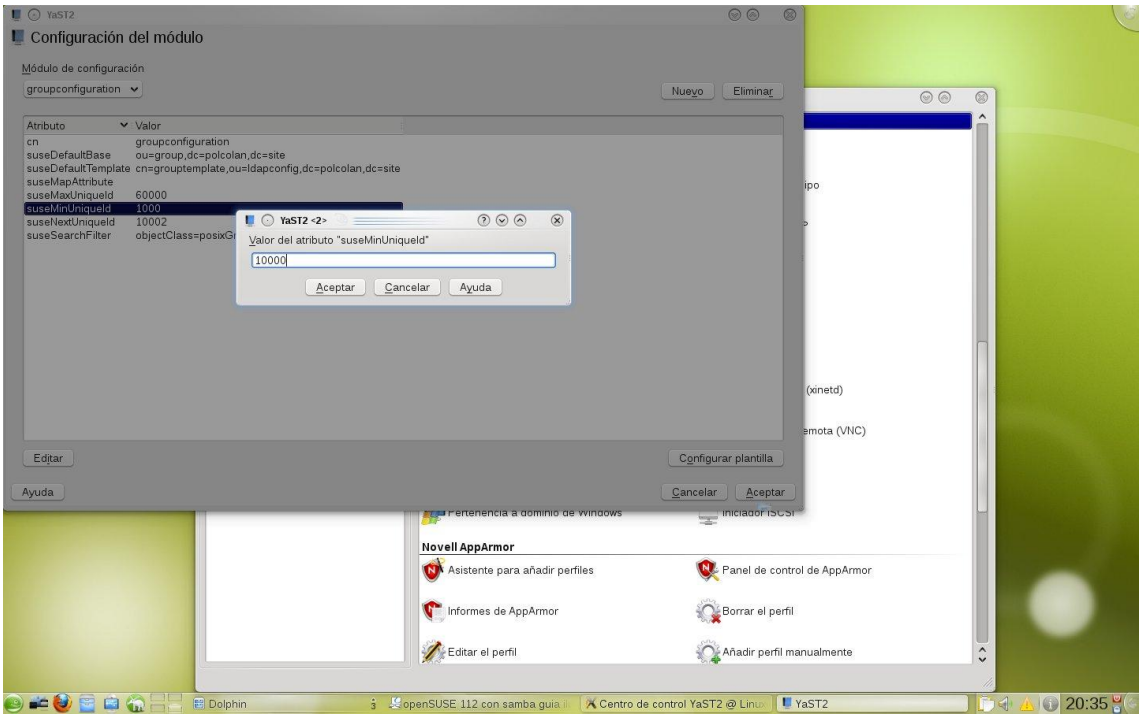
- Luego de realizar las configuraciones mencionadas nos solicitara la clave de del administrador del servidor LDAP, haga clic en **Aceptar** para dejar la configuración avanzada y a continuación, en **Finalizar** para aplicar los ajustes.

6.2.2.2. Configuración de los módulos de administración de usuarios y grupos de YaST

Utilice el cliente LDAP de YaST para adaptar los módulos de YaST a la administración de usuarios y grupos y para ampliarlos si fuera necesario. Defina las plantillas con los valores por defecto para los atributos individuales con objeto de simplificar el registro de datos. Los ajustes predefinidos creados aquí se almacenarán como objetos LDAP en el directorio LDAP. El registro de los datos de usuario se seguirá realizando con los módulos de YaST habituales para la gestión de usuarios y grupos. Los datos registrados se almacenan como objetos LDAP en el servidor.

Configuración de módulos





El cuadro de diálogo para la configuración de módulos, permite la creación de módulos nuevos, la selección y modificación de los módulos de configuración existentes y el diseño y la modificación de plantillas para tales módulos.

Para crear un módulo nuevo de configuración, actúe de la siguiente manera:

- Haga clic en ‘Nuevo’ y seleccione el tipo de módulo que crear. En el caso de un módulo de configuración de usuarios, seleccione userconfiguration y para la configuración de grupos groupconfiguration.
- Seleccione un nombre para la plantilla nueva.
- La vista del contenido presenta a continuación una tabla con todos los atributos permitidos en este módulo junto con los valores asignados. Aparte de todos los atributos definidos, la lista también contiene todos los atributos permitidos por el esquema actual pero que no están actualmente en uso.
- Acepte los valores predefinidos o ajuste los valores por defecto para usarlos en la configuración de usuarios y de grupos seleccionando el atributo respectivo, pulsando ‘Editar’ e introduciendo un valor nuevo. Cámbiele el nombre al módulo, simplemente modificando el atributo cn. Al hacer clic en ‘Suprimir’ se suprime el módulo seleccionado.
- Después de hacer clic en ‘Aceptar,’ se añade el nuevo módulo al menú de selección.

Los módulos de YaST para la administración de usuarios y grupos incrustan plantillas con valores estándar razonables. Para editar una plantilla asociada con un módulo de configuración, actúe de la siguiente manera:

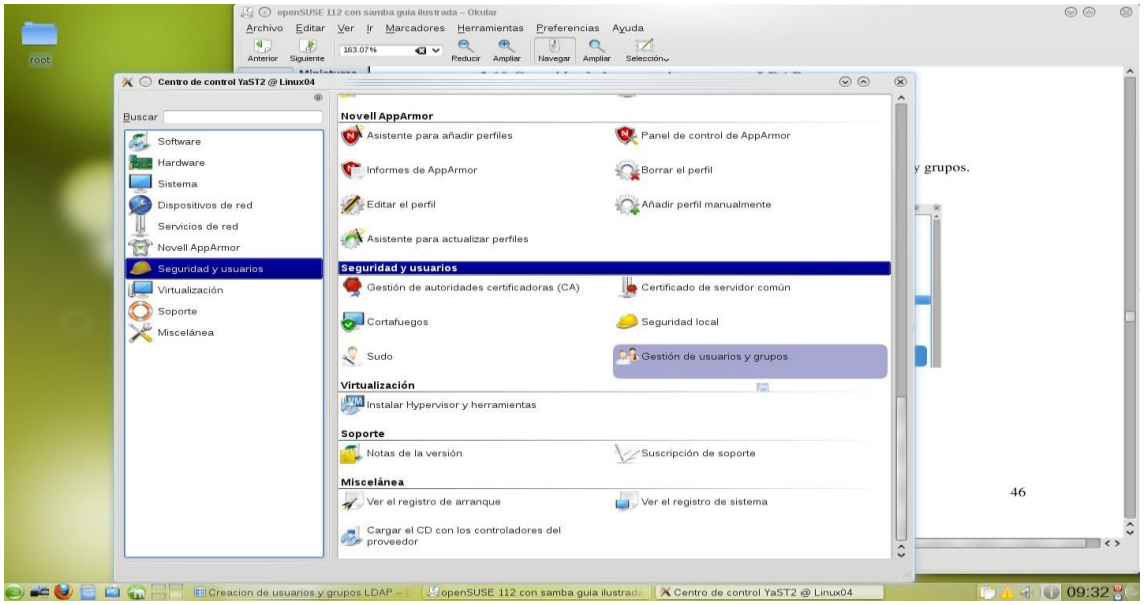
1. En el cuadro de diálogo ‘Configuración del módulo,’ haga clic en ‘Configurar plantilla.’
2. Determine los valores de los atributos generales asignados a esta plantilla según sus necesidades o deje algunos vacíos. Los atributos vacíos se suprimen del servidor LDAP.
3. Modifique, suprima o añada nuevos valores por defecto para los nuevos objetos (objetos de configuración de usuarios y grupos en el árbol LDAP).

Una vez que todos los módulos y plantillas se han configurado correctamente y están listos para funcionar, los nuevos grupos y usuarios se pueden registrar con YaST de la manera habitual.

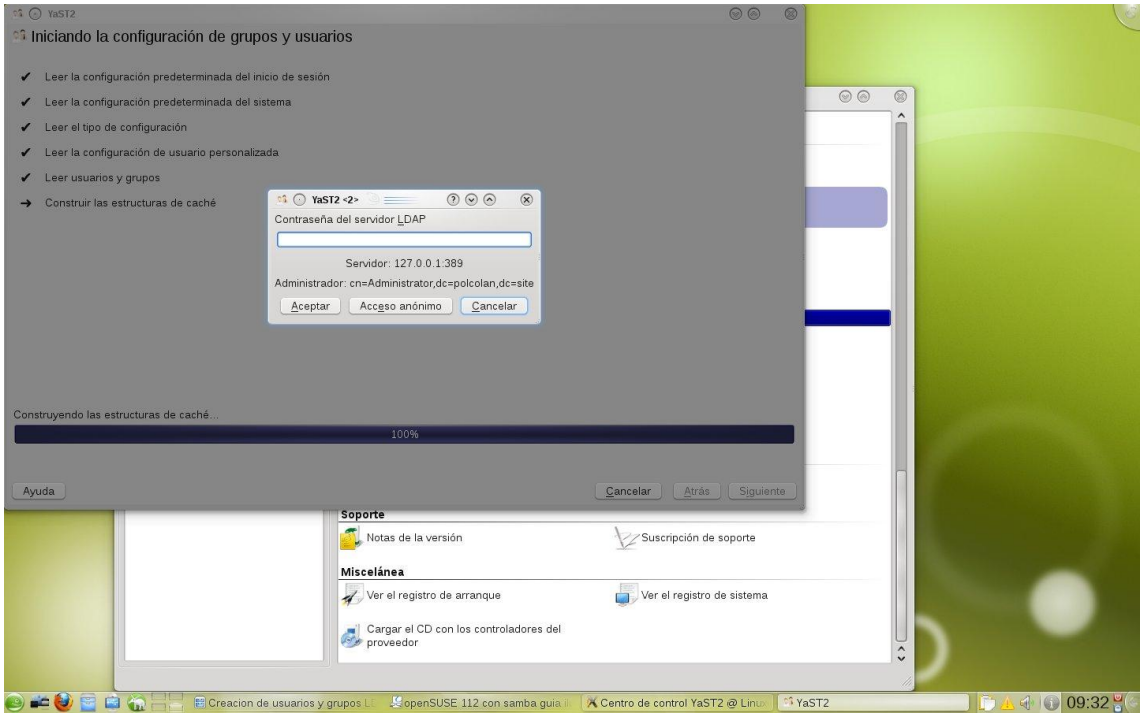
6.3. CONFIGURACIÓN DE LOS USUARIOS Y GRUPOS LDAP EN YAST

El registro real de los datos de usuario y de grupo difiere sólo un poco del procedimiento cuando no se usa LDAP. Las siguientes instrucciones tienen que ver con la administración de usuarios. El procedimiento para administrar grupos es análogo.

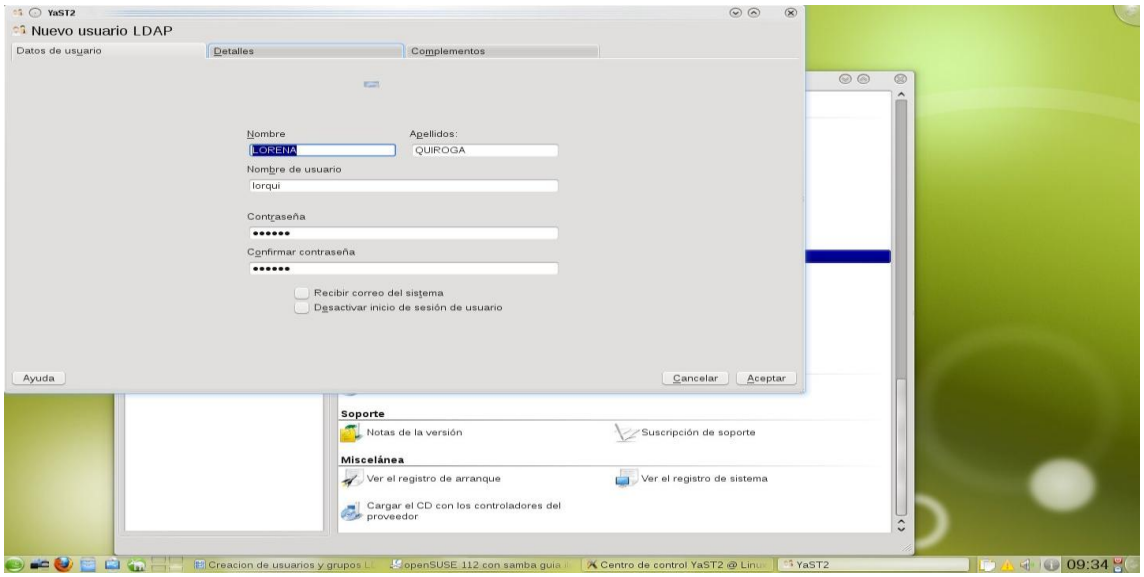
- Acceda a la administración de usuarios de YaST mediante Seguridad y usuarios / Gestión de usuario y grupos.



- Nos solicitara la contraseña del administrador del servidor LDAP para comenzar con la configuración Utilice Definir filtro para limitar la visualización de usuarios a los usuarios de LDAP e introduzca la contraseña para el DN raíz.

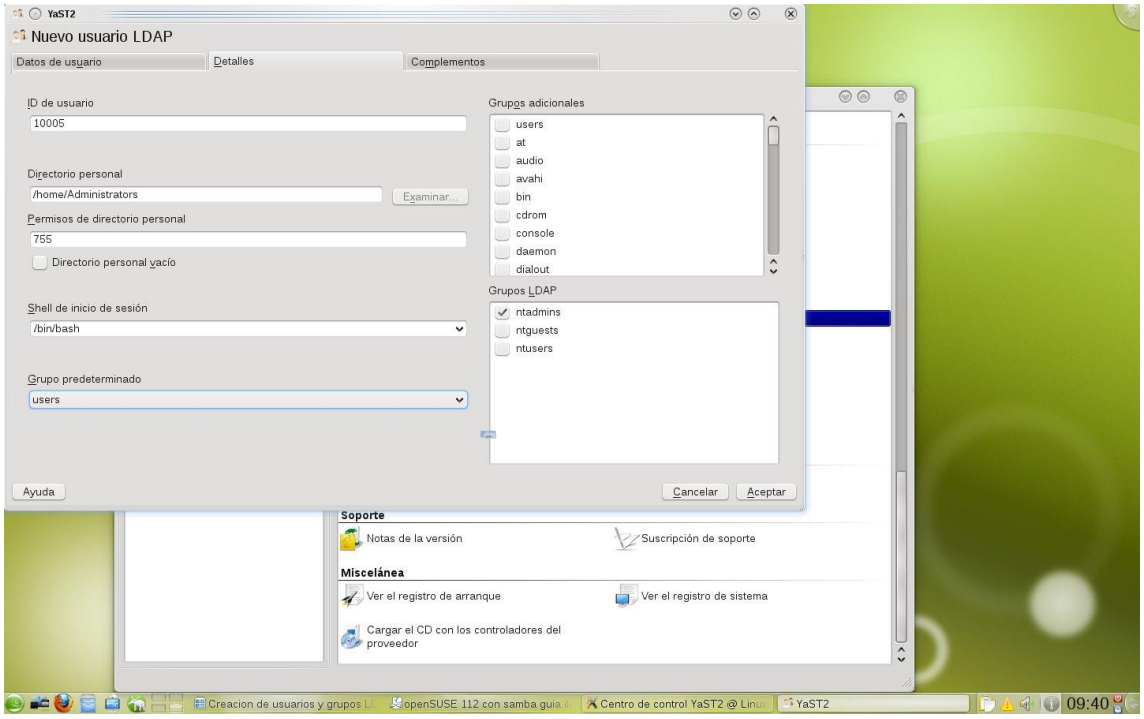


- Haga clic en Añadir e introduzca la configuración de un usuario nuevo. Se abrirá un cuadro de diálogo con cuatro pestañas:
  - ✓ Especifique el nombre de usuario, inicio de sesión y contraseña en la pestaña ‘Datos de usuario.’



  - ✓ Compruebe la pestaña ‘Detalles’ para los miembros de grupo, shell de inicio de sesión y directorio personal del nuevo usuario. Si fuera necesario, cambie el valor por defecto a otros que se ajusten mejor a sus necesidades. Los valores por defecto y los ajustes de contraseña se pueden definir con el procedimiento descrito en la

Sección Configuración de los módulos de administración de usuarios y grupos de YaST".



- ✓ Haga clic en 'Aceptar' para aplicar los ajustes y abandonar la configuración del usuario.

7. GLOSARIO

- **LDAP:** Lightweight Directory Access Protocol
- **GNU:** General Public License
- **Slapd.conf:** archivo de configuración para especificar el dominio y servidor.
- **Queries:** es una consulta de datos en una tabla perteneciente a una base de datos.
- **TCP/IP:** Transmission Control Protocol / Protocolo de control de transmisión
- **SSL:** Secure Socket Layer
- **FTP:** File Transfer Protocol
- **LDIF:** LDAP Data Interchange Format (LDIF) es un formato que se utiliza para la importación y exportación de datos independientemente del servidor LDAP que se esté utilizando.
- **RAID:** Redundant Array of Independent Disks, «conjunto redundante de discos independientes

8. CONCLUSIONES

- Un servidor LDAP es una excelente alternativa de control de acceso a los recursos de una compañía cuando no se tienen suficientes recursos económicos o tecnológicos.

- OpenLDAP nos muestra la facilidad de implementar recursos con software GNU.

- De manera rápida y sencilla se puede realizar la instalación, configuración y administración de un servidor OpenLDAP.

- OpenSUSE y OpenLDAP son dos herramientas muy fáciles de utilizar ya que su funcionalidad es muy versátil y permite interactuar de lleno con sus mejores características.

9. BIBLIOGRAFIA

- Manual de OpenLDAP en español: http://www.ldap-es.org/node/20
- OpenLDAP – Wikipedia: http://es.wikipedia.org/wiki/OpenLDAP
- ESLINUX: http://www.eslinux.com/foro/3829/que-openldap
- OpenLDAP: www.openldap.org
- OpenLDAP - OpenSUSE: http://en.opensuse.org/OpenLDAP
- Howto setup SUSE as SAMBA PDC with OpenLDAP, DYNDNS and CLAM: http://es.opensuse.org/Howto_setup_SUSE_as_SAMBA_PDC_with_OpenLDAP,_DYNDNS_and_CLAM
- Wikipedía, enciclopedia libre: http://www.wikipedia.org
- Buscador: http://www.google.com.co